WHAT IS CLAIMED IS:

1. A method for secure data transmission, comprising:

generating a character string at a sender;

generating a hash key using the character string and a private key;

encrypting the data using the hash key; and

transmitting an identification key associated with the sender, the character string, and the encrypted data from the sender to a recipient.

2. The method of Claim 1, wherein generating the hash key comprises hashing the character string with the private key.

3. The method of Claim 1, further comprising:

generating a signature using the hash key and the data; and

transmitting the signature from the sender to the recipient.

4. The method of Claim 1, wherein generating a character string comprises randomly generating the character string.

5. The method of Claim 1, further comprising:

determining the private key at the recipient using the identification key; and

decrypting the encrypted data at the recipient using the private key and the character string.

6. The method of Claim 5, wherein determining the private key comprises accessing a relational database associating the identification key to the private key.

7. The method of Claim 1, further comprising:

determining the private key at the recipient using the identification key;

determining the hash key at the recipient using the private key and the character string; and

decrypting the encrypted data using the hash key.

8. The method of Claim 7, wherein determining the hash key comprises hashing the private key with the character string.

9. The method of Claim 1, further comprising:

generating a first signature by the sender using the hash key and the data; and

transmitting the first signature to the recipient, the recipient adapted to determine the hash key for decrypting the data and compare the first signature to a second signature generated by the recipient using the hash key and the decrypted data.

10. The method of Claim 1, further comprising:

generating a signature using the hash key and the data;

transmitting the signature to the recipient;

determining the private key at the recipient using the identification key;

determining the hash key at the recipient using the private key and the character string;

decrypting the encrypted data at the recipient using the hash key; and

verifying the signature at the recipient using the hash key and the decrypted data.

11. A method for secure data transmission, comprising:

receiving a character string from a sender;

receiving an identification key from the sender;

receiving encrypted data from the sender;

determining a private key associated with the sender using the identification key; and

decrypting the encrypted data using the private key and the character string.

12. The method of Claim 11, further comprising determining a hash key using the character string and the private key, and wherein decrypting the encrypted data comprises decrypting the encrypted data using the hash key.

13. The method of Claim 11, wherein determining the private key comprises accessing a relational database associating the identification key to the private key.

14. The method of Claim 11, wherein receiving the character string comprises receiving a randomly generated character string.

15. The method of Claim 11, further comprising hashing the character string with the private key to generate a hash key, and wherein decrypting the encrypted data comprises decrypting the encrypted data using the hash key.

16. The method of Claim 11, further comprising:

receiving a signature from the sender; and

verifying the signature using the decrypted data, the private key, and the character string.

17. The method of Claim 11, further comprising:

receiving a signature from the sender;

determining a hash key using the private key and the character string; and

verifying the signature using the decrypted data and the hash key.

18. The method of Claim 11, further comprising:

receiving a first signature from the sender;

determining a hash key using the private key and the character string;

generating a second signature using the hash key and the decrypted data; and

comparing the first signature to the second signature.